

EXTREMAL PRODUCT-ONE FREE SEQUENCES IN DIHEDRAL AND DICYCLIC GROUPS

F. E. BROCHERO MARTÍNEZ AND SÁVIO RIBAS

ABSTRACT. Let G be a finite group, written multiplicatively. The Davenport constant of G is the smallest positive integer $D(G)$ such that every sequence of G with $D(G)$ elements has a non-empty subsequence with product 1. Let D_{2n} be the Dihedral Group of order $2n$ and Q_{4n} be the Dicyclic Group of order $4n$. J. J. Zhuang and W. Gao [19] showed that $D(D_{2n}) = n + 1$ and J. Bass [2] showed that $D(Q_{4n}) = 2n + 1$. In this paper, we give explicit characterizations of all sequences S of G such that $|S| = D(G) - 1$ and S is free of subsequences whose product is 1, where G is equal to D_{2n} or Q_{4n} for some n .

1. INTRODUCTION

Given a finite group G written multiplicatively, the *Zero-Sum Problems* study conditions that guarantee a non-empty subsequence in G has a non-empty subsequence with certain prescribed properties such that the product of its elements, in some order, is equal to the identity $1 \in G$. Interesting properties include length, repetitions, and weights.

One of the first problem of this type was considered by Erdős, Ginzburg, and Ziv [6]. They proved that given $2n - 1$ integers, it is possible to select n of them, such that their sum is divisible by n . In the language of group theory, every sequence S consisting of at least $2n - 1$ elements in a finite cyclic group of order n has a subsequence T of length n such that the product of the elements in T in some order is equal to the identity. Further, they proved that the number $2n - 1$ is the smallest positive integer with this property.

These problems have been studied extensively for abelian groups; see the surveys by Y. Caro [5] and W. Gao - A. Geroldinger [9].

An important problem of zero-sum type is to determine the so-called *Davenport constant* of a finite group G (written multiplicatively). This constant, denoted by $D(G)$, is the smallest positive integer d such that every sequence S with d elements in G (repetition allowed) contains some subsequence T such that the product of the elements in T in some order is 1.

For $n \in \mathbb{N}$, let $C_n \simeq \mathbb{Z}_n$ denote the cyclic group of order n written multiplicatively. The Davenport constant is known for the following groups:

- $D(C_n) = n$;
- $D(C_m \times C_n) = m + n - 1$ if $m|n$ (J. Olson, [14]);
- $D(C_{p^{e_1}} \times \cdots \times C_{p^{e_r}}) = 1 + \sum_{i=1}^r (p^{e_i} - 1)$ (J. Olson, [13]);
- $D(D_{2n}) = n + 1$ where D_{2n} is the Dihedral Group of order $2n$ (see [19]);
- $D(C_q \rtimes_s C_m) = m + q - 1$ where $q \geq 3$ is a prime number and $\text{ord}_q(s) = m \geq 2$ (J. Bass, [2]).

For most finite groups, the Davenport constant is not known.

By the definition of the Davenport constant, for a given finite group G there exist sequences S with elements in G such that $|S| = D(G) - 1$ and such that S is *free of product-1 subsequences*. That is, there exists $S = (g_1, \dots, g_{D(G)-1})$ of G such that $g_{i_1} \cdots g_{i_k} \neq 1$ for every non-empty subset $\{i_1, \dots, i_k\}$ of $\{1, \dots, D(G) - 1\}$. The *Inverse Zero-Sum Problems* study the structure of these extremal-length sequences which are free of product-1 subsequences with some prescribed property. For an overview, see articles by W. Gao, A. Geroldinger, D. J. Grynkiewicz and W. A. Schmid [11], [16] and [10].

The inverse problems associated with Davenport constant are solved for few abelian groups. For example, the following theorem is direct consequence of Theorem 2.2 and gives a complete characterization of sequences free of product-1 subsequences in the finite cyclic group C_n .

Theorem 1.1. *Let S be a sequence in C_n free of product-1 subsequences with $n - 1$ elements, where $n \geq 2$. Then*

$$S = (\underbrace{g, \dots, g}_{n-1 \text{ times}}), \text{ where } g \text{ is a generator of } C_n.$$

Date: February 1, 2017.

2010 *Mathematics Subject Classification.* 20D60 (primary) and 11P70 (secondary).

Key words and phrases. Zero-sum problem, Davenport constant, inverse zero-sum.

Observe that in the cyclic case, sequences free of product-1 subsequences contain an element repeated many times. It is natural to ask if this is true in general. Specifically, let us say that a given finite abelian group G has *Property C* if every maximal sequence S of G free of product-1 subsequences with at most $\exp(G)$, the exponent of the group G , elements has the form

$$S = (\underbrace{T, T, \dots, T}_{\exp(G)-1 \text{ times}}),$$

for some subsequence T of S . The above theorem states that C_n has Property C. It then follows from a result of C. Reiher [15] that C_p^2 possesses Property C (see also [11] and [8]). In [10], W. Gao, A. Geroldinger and D. J. Grynkiewicz showed that this result is multiplicative, extending our conclusion to the groups C_n^2 for a composite number n . In [17], W. A. Schmid discusses the case $C_n \times C_m$, where $n|m$. Not much is known about groups of rank exceeding 2, only few specific cases (see, for example, [17]).

A *minimal zero sequence* S in a finite abelian group G is a sequence such that the product of its elements is 1, but each proper subsequence is free of product-1 subsequences. In [7, Theorem 6.4], W. Gao and A. Geroldinger showed that if $|S| = D(G)$ then S contains some element $g \in G$ with order $\text{ord}(g) = \exp(G)$ for certain groups such as p -groups, cyclic groups, groups with rank two and groups that are the sum of two elementary p -groups. They also conjectured that the same conclusion holds for every finite abelian group.

For non-abelian groups, nothing was known, until the paper [4] where we solved the inverse problem associated to the metacyclic group

$$C_q \rtimes_s C_m = \langle x, y | x^m = 1, y^q = 1, yx = xy^s, \text{ord}_q(s) = m, q \text{ prime} \rangle.$$

Specifically, we proved the following result:

Theorem 1.2 ([4, Theorem 1.2]). *Let q be a prime number, $m \geq 2$ be a divisor of $q - 1$ and $s \in \mathbb{Z}_q^*$ such that $\text{ord}_q(s) = m$.*

Let S be a sequence in the metacyclic group $C_q \rtimes_s C_m$ with $m + q - 2$ elements.

(1) *If $(m, q) \neq (2, 3)$ then the following statements are equivalent:*

(i) *S is free of product-1 subsequences;*

(ii) *For some $1 \leq t \leq q - 1$, $1 \leq i \leq m - 1$ such that $\gcd(i, m) = 1$ and $0 \leq \nu_1, \dots, \nu_{m-1} \leq q - 1$,*

$$S = (\underbrace{y^t, y^t, \dots, y^t}_{q-1 \text{ times}}, x^i y^{\nu_1}, x^i y^{\nu_2}, \dots, x^i y^{\nu_{m-1}}).$$

(2) *If $(m, q) = (2, 3)$ then S is free of product-1 subsequences if and only if*

$$S = (y^t, y^t, xy^\nu) \text{ for } t \in \{2, 3\} \text{ and } \nu \in \{0, 1, 2\} \quad \text{or} \quad S = (x, xy, xy^2).$$

In this article, we characterize the maximal sequences which are free of product-1 subsequences for the *Dihedral Groups* and the *Dicyclic Groups*. In particular, we show that these sequences have a property similar to Property C.

Let $n \geq 2$. Denote by $D_{2n} \simeq C_n \rtimes_{-1} C_2$ the *Dihedral Group* of order $2n$, i.e., the group generated by x and y with relations:

$$x^2 = y^n = 1, \quad yx = xy^{-1}.$$

Let $n \geq 2$. Denote by Q_{4n} the *Dicyclic Group*, i.e., the group generated by x and y with relations:

$$x^2 = y^n, \quad y^{2n} = 1, \quad yx = xy^{-1}.$$

We have $Z(Q_{4n}) = \{1, y^n\}$, where $Z(G)$ denotes the center of a group G . In addition:

$$Q_{4n}/\{1, y^n\} \simeq D_{2n},$$

where D_{2n} is the Dihedral Group of order $2n$.

Specifically, we prove the following result:

Theorem 1.3. *Let S be a sequence in the Dihedral Group D_{2n} with n elements, where $n \geq 3$.*

(1) *If $n \geq 4$ then the following statements are equivalent:*

(i) *S is free of product-1 subsequences;*

(ii) *For some $1 \leq t \leq n - 1$ with $\gcd(t, n) = 1$ and $0 \leq s \leq n - 1$,*

$$S = (\underbrace{y^t, y^t, \dots, y^t}_{n-1 \text{ times}}, xy^s).$$

(2) *If $n = 3$ then S is free of product-1 subsequences if and only if*

$$S = (y^t, y^t, xy^\nu) \text{ for } t \in \{2, 3\} \text{ and } \nu \in \{0, 1, 2\} \quad \text{or} \quad S = (x, xy, xy^2).$$

Notice that this theorem reduces to Theorem 1.2 in the case when n is prime and when $m = 2$, since we have $s \equiv -1 \pmod{n}$. For $n \geq 4$, it is easy to check that (ii) \implies (i). Observe that the case $n = 3$ is exactly the item (2) of Theorem 1.2, since $D_6 \simeq C_3 \rtimes_{-1} C_2$. For $n = 2$, we have $D_4 \simeq \mathbb{Z}_2^2$ and it is easy to check that S is free of product-1 subsequences if and only if $S = (x, y)$, $S = (xy, y)$ or $S = (x, xy)$.

As a consequence of previous theorem, we obtain:

Theorem 1.4. *Let S be a sequence in the Dicyclic Group Q_{4n} with $2n$ elements, where $n \geq 2$.*

(1) *If $n \geq 3$ and $|S| = 2n$ then the following statements are equivalent:*

- (i) *S is free of product-1 subsequences;*
- (ii) *For some $1 \leq t \leq n-1$ with $\gcd(t, 2n) = 1$ and $0 \leq s \leq 2n-1$,*

$$S = \underbrace{(y^t, y^t, \dots, y^t)}_{2n-1 \text{ times}}, xy^s).$$

(2) *If $n = 2$ then S is free of product-1 subsequences if and only if, for some $r \in \mathbb{Z}_4^*$ and $s \in \mathbb{Z}_4$, S has one of the forms*

$$(y^r, y^r, y^r, xy^s), (y^r, xy^s, xy^s, xy^s) \text{ or } (xy^s, xy^s, xy^s, xy^{r+s}).$$

Again, if $n \geq 3$ then it is easy to check that (ii) \implies (i), therefore we just need to show that (i) \implies (ii). If $n = 2$ then it is easy to check that the sequences of the form (y^r, y^r, y^r, xy^s) , (y^r, xy^s, xy^s, xy^s) , $(xy^s, xy^s, xy^s, xy^{r+s})$ are free of product-1 subsequences, therefore we just need to show that all other sequences with $2n$ elements have subsequences with product 1.

Also note that if $n = 2$ then Q_8 is isomorphic to the *Quaternion Group*, i.e. the group defined by

$$\langle e, i, j, k \mid i^2 = j^2 = k^2 = ijk = e, e^2 = 1 \rangle.$$

This isomorphism may be described, for example, by $x \mapsto i, y \mapsto j$ (or its natural permutations, by the symmetry of i, j, k). The above theorem says that, in terms of Quaternion Group, extremal sequences free of product-1 subsequence are of the forms

$$\pm(i, i, i, \pm j), \pm(i, i, i, \pm k), \pm(j, j, j, \pm i), \pm(j, j, j, \pm k), \pm(k, k, k, \pm i) \text{ or } \pm(k, k, k, \pm j).$$

The main technical difficulty in our present proofs lies on the fact that n may not be prime, therefore we cannot use Cauchy-Davenport inequality (see [12, p. 44-45]) and Vosper's Theorem (see [18]), as used in the proof of Theorem 1.2 (see [4]). Instead, we now exhibit sequences with product-1 in cases not covered by those given forms. In section 3 we prove Theorem 1.3, solving the extremal inverse zero-sum problem associated to Davenport constant for dihedral groups. The proof of Theorem 1.4 is split up into sections 4, 5 and 6, where we solve the extremal inverse zero-sum problem associated to Davenport constant for dicyclic groups of orders $4n$, where $n \geq 4$, $n = 3$ and $n = 2$, respectively. The case $n \geq 4$ is a direct consequence of Theorem 1.3 and the case $n = 3$ follows from Theorem 1.3, but in the special case (2). The proof in the case $n = 2$ is done manually, using only Theorem 2.2 to reduce the number of cases, without using Theorem 1.3.

2. NOTATION AND AUXILIARY RESULTS

In this section we present the notation and auxiliary lemmas and theorems that we use throughout the paper.

Let G be a finite group written multiplicatively and $S = (g_1, g_2, \dots, g_l)$ be a sequence of elements of G . We denote by $|S| = l$ the length of S .

For each subsequence T of S , i.e. $T = (g_{n_1}, g_{n_2}, \dots, g_{n_k})$, where $\{n_1, n_2, \dots, n_k\}$ is a subset of $\{1, 2, \dots, l\}$, we say that T is a *product-1 subsequence* when

$$g_{\sigma(n_1)} g_{\sigma(n_2)} \cdots g_{\sigma(n_k)} = 1$$

for some permutation σ of $\{n_1, \dots, n_k\}$, and if there are no such product-1 subsequences then we say that S is *free of product-1 subsequences*.

If $S_1 = (g_{i_1}, \dots, g_{i_u})$ and $S_2 = (g_{j_1}, \dots, g_{j_v})$ are subsequences of S , then

- SS_1^{-1} denotes the subsequence formed by the elements of S without the elements of S_1 ;
- $S_1 S_2 = (g_{i_1}, \dots, g_{i_u}, g_{j_1}, \dots, g_{j_v})$ denotes the concatenation of S_1 and S_2 ;
- $S^k = SS \dots S$ denotes the concatenation of k identical copies of S 's.

For the group $G = D_{2n} = \langle x, y \mid x^2 = 1, y^n = 1, yx = xy^{-1} \rangle$, let

- H_D be the normal cyclic subgroup of order n generated by y ;
- $N_D = D_{2n} \setminus H_D = x \cdot H_D$.

The product of any even number of elements in N_D is in H_D , since

$$xy^\alpha \cdot xy^\beta = y^{\beta-\alpha}. \quad (2.1)$$

For the group $G = Q_{4n} = \langle x, y | x^2 = y^n, y^{2n} = 1, yx = xy^{-1} \rangle$, let

- H_Q be the normal cyclic subgroup of order $2n$ generated by y ;
- $N_Q = Q_{4n} \setminus H_Q = x \cdot H_Q$.

The product of any even number of elements in N_Q is in H_Q , since

$$xy^\alpha \cdot xy^\beta = y^{\beta-\alpha+n}. \quad (2.2)$$

The following theorem is known as “Davenport constant of \mathbb{Z}_n with weights $\{\pm 1\}$ ”, and will be used in the proof of Theorem 1.3.

Lemma 2.1 ([1, Lemma 2.1]). *Let $n \in \mathbb{N}$ and (y_1, \dots, y_s) be a sequence of integers with $s > \log_2 n$. Then there exist a nonempty $J \subset \{1, 2, 3, \dots, s\}$ and $\varepsilon_j \in \{\pm 1\}$ for each $j \in J$ such that*

$$\sum_{j \in J} \varepsilon_j y_j \equiv 0 \pmod{n}.$$

As a generalization of Theorem 1.1, we will use the following:

Theorem 2.2 ([11, Theorem 2.1], see also [3]). *Let G be a cyclic group of order $n \geq 3$ and S be a zero-sum free sequence in G of length $|S| \geq (n+1)/2$. Then there exists some $g \in S$ that appear at least $2|S| - n + 1$ times in S . In particular, $D(G) = n$ and the following statements hold:*

- (1) *If $|S| = n - 1$, then $S = (g)^{n-1}$.*
- (2) *If $|S| = n - 2$, then either $S = (g)^{n-2}$ or $S = (g)^{n-3}(g^2)$.*
- (3) *If $|S| = n - 3$, then S has one of the following forms:*

$$(g)^{n-3}, (g)^{n-4}(g^2), (g)^{n-4}(g^3), (g)^{n-5}(g^2)^2.$$

3. PROOF OF THEOREM 1.3

We just need to show that (i) \implies (ii). Let S be a sequence in D_{2n} with n elements that is free of product-1 subsequences. If $S \cap N_D$ contains two identical elements then S is not free of product-1 subsequences by Equation 2.1. Hence, we assume that the elements of $S \cap N_D$ are all distinct.

From now on, we consider some cases, depending on the cardinality of $S \cap H_D$:

- Case $|S \cap H_D| = n$:** In this case, S is contained in the cyclic subgroup of order n . Since $D(\mathbb{Z}_n) = n$, S contains some non-empty subsequence with product 1.
- Case $|S \cap H_D| = n - 1$:** In this case, by Theorem 2.2, the elements of $S \cap H_D$ must all be equal, say, $S \cap H_D = (y^t)^{n-1}$ where $\gcd(t, n) = 1$, and so $S = (y^t)^{n-1}(xy^s)$.
- Case $|S \cap H_D| = n - 2$:** In this case, by Theorem 2.2, S must have one of these forms:
 - Subcase $S = (y^t)^{n-2}(xy^u, xy^v)$:** Notice that we can obtain the products

$$xy^u \cdot \underbrace{y^t \cdot y^t \dots y^t}_{k \text{ times}} \cdot xy^v = y^{v-u-kt}.$$

Since $1 \leq k \leq n - 2$, it's enough to take $k \equiv (v - u)t^{-1} \pmod{n}$. The only problem occurs when $k = n - 1$, that is, when $v - u + t \equiv 0 \pmod{n}$, but in this case we switch u and v and so

$$xy^v \cdot y^t \cdot xy^u = y^{u-v-t} = 1.$$

- Subcase $S = (y^t)^{n-3}(y^{2t}, xy^u, xy^v)$:** Notice that we can obtain the products

$$xy^u \cdot \underbrace{y^t \cdot y^t \dots y^t}_{k \text{ times}} \cdot xy^v = y^{v-u-kt}.$$

Since $1 \leq k \leq n - 1$, it's enough to take $k \equiv (v - u)t^{-1} \pmod{n}$.

- (d) **Case** $|S \cap H_D| = n - 3$: In this case, by Theorem 2.2, S must contain at least $n - 5$ copies of some y^t , where $\gcd(t, n) = 1$. Also, suppose that

$$S \cap N_D = (xy^\alpha, xy^\beta, xy^\gamma).$$

By renaming $z = y^t$, we may assume without loss of generality that $t = 1$. By Pigeonhole Principle it follows that there exist two exponents of y with difference in $\{1, 2, \dots, \lfloor n/3 \rfloor\} \pmod{n}$, say,

$$\alpha - \beta \in \{0, 1, 2, \dots, \lfloor n/3 \rfloor\} \pmod{n}.$$

We may ensure that

$$xy^\beta \cdot y^r \cdot xy^\alpha = y^{\alpha-\beta-r} = 1$$

for some $1 \leq r \leq n/3$ provided there are enough y 's. But if $n \geq 8$ then $r \leq n/3 \leq n - 5$, so there are enough y 's and the theorem follows in these cases. Since the theorem is already proved for n prime, it only remains to prove for $n \in \{4, 6\}$.

For $n = 4$, we have $S = (xy^\alpha, xy^\beta, xy^\gamma, y)$ and some of the α, β, γ are consecutives modulo 4. Without loss of generality, suppose that $\alpha - \beta \equiv 1 \pmod{4}$, so $xy^\beta \cdot y \cdot xy^\alpha = 1$.

For $n = 6$, we have the cases

$$\begin{cases} S = (xy^\alpha, xy^\beta, xy^\gamma, y, y, y); \\ S = (xy^\alpha, xy^\beta, xy^\gamma, y, y, y^2); \\ S = (xy^\alpha, xy^\beta, xy^\gamma, y, y, y^3); \text{ or} \\ S = (xy^\alpha, xy^\beta, xy^\gamma, y, y^2, y^2). \end{cases}$$

If the set $\{\alpha, \beta, \gamma\} \pmod{6}$ contains two consecutive elements, say $\alpha \equiv \beta + 1 \pmod{6}$, then

$$xy^\alpha \cdot xy^\beta \cdot y = y^{\beta+1-\alpha} = 1.$$

Otherwise, the only possibilities are $\{\alpha, \beta, \gamma\} \pmod{6} = \{0, 2, 4\}$ or $\{\alpha, \beta, \gamma\} \pmod{6} = \{1, 3, 5\}$. Suppose that $\alpha \equiv \beta + 2 \pmod{6}$ and notice that in any option for S it is possible to take a product y^2 coming from $S \cap H_D$. Therefore

$$xy^\alpha \cdot xy^\beta \cdot y^2 = y^{\beta+2-\alpha} = 1.$$

- (e) **Case** $|S \cap H_D| = n - k, 4 \leq k \leq n$: Suppose that

$$\begin{aligned} S \cap H_D &= (y^{t_1}, y^{t_2}, \dots, y^{t_{n-k}}), \\ S \cap N_D &= (xy^{\alpha_1}, xy^{\alpha_2}, \dots, xy^{\alpha_k}). \end{aligned}$$

It follows from Theorem 2.1 that if

$$\lfloor k/2 \rfloor > \lfloor \log_2 n \rfloor \tag{3.1}$$

then there exist a linear combination of a subset of

$$\{(\alpha_1 - \alpha_2), (\alpha_3 - \alpha_4), \dots, (\alpha_{2\lfloor k/2 \rfloor - 1} - \alpha_{2\lfloor k/2 \rfloor})\}$$

with coefficients ± 1 summing 0. Suppose without loss of generality that, in this combination,

$$(\alpha_1 - \alpha_2), (\alpha_3 - \alpha_4), \dots, (\alpha_{2u-1} - \alpha_{2u})$$

appear with signal -1 and

$$(\alpha_{2u+1} - \alpha_{2u+2}), (\alpha_{2u+3} - \alpha_{2u+4}), \dots, (\alpha_{2v-1} - \alpha_{2v}),$$

appear with signal $+1$. Then

$$\begin{aligned} (xy^{\alpha_1} \cdot xy^{\alpha_2}) \dots (xy^{\alpha_{2u-1}} \cdot xy^{\alpha_{2u}}) \cdot (xy^{\alpha_{2u+1}} \cdot xy^{\alpha_{2u+2}}) \cdot (xy^{\alpha_{2v-1}} \cdot xy^{\alpha_{2v}}) = \\ y^{\alpha_2 - \alpha_1} \dots y^{\alpha_{2u} - \alpha_{2u-1}} \cdot y^{\alpha_{2u+1} - \alpha_{2u+2}} \dots y^{\alpha_{2v-1} - \alpha_{2v}} = 1 \end{aligned}$$

Thus the theorem is true for $k > 2\lfloor \log_2 n \rfloor + 1$.

Hence, we may assume $4 \leq k \leq 2\lfloor \log_2 n \rfloor + 1$. Theorem 2.2 implies without loss of generality that $t_i = t$ for $1 \leq i \leq n - 2k + 1$. By renaming $z = y^t$, we may assume without loss of generality that $t = 1$. Since $k \geq 4$, Pigeonhole Principle implies that there exist α_i, α_j such that

$$\alpha_i - \alpha_j \in \{1, 2, \dots, \lfloor n/4 \rfloor\}.$$

Notice that if

$$n - 2k + 1 \geq n/4 \tag{3.2}$$

then

$$xy^{\alpha_j} \cdot y^r \cdot xy^{\alpha_i} = y^{\alpha_i - \alpha_j - r} = 1$$

for some $0 \leq r \leq \lfloor n/4 \rfloor$. But if $n \geq 8$ then $3n \geq 8 \log_2 n \geq 4(k-1)$, therefore Equation 3.2 holds in this case. Since the theorem is already proved for n prime, it only remains to prove for $n \in \{4, 6\}$.

For $n = 4$, the only possibility is $S = (x, xy, xy^2, xy^3)$. Thus, $x \cdot xy \cdot xy^3 \cdot xy^2 = 1$.

For $n = 6$, there are three subcases to consider:

- **Subcase $k = 4$:** Let $S = (y^{t_1}, y^{t_2}, xy^{\alpha_1}, xy^{\alpha_2}, xy^{\alpha_3}, xy^{\alpha_4})$. Then either there are two pairs of consecutive α_i 's modulo 6 or there are three consecutive α_i 's modulo 6.
 - If there are two pairs of consecutive α_i 's, say $\alpha_1 + 1 \equiv \alpha_2$ and $\alpha_3 + 1 \equiv \alpha_4 \pmod{6}$, then

$$xy^{\alpha_1} \cdot xy^{\alpha_2} \cdot xy^{\alpha_4} \cdot xy^{\alpha_3} = 1.$$

- If there are three consecutive α_i 's, say $\alpha_1 + 2 \equiv \alpha_2 + 1 \equiv \alpha_3 \pmod{6}$, then α_4 can be any element in the set $\{\alpha_3 + 1, \alpha_3 + 2, \alpha_3 + 3\}$. If $\alpha_4 \equiv \alpha_3 + 1$ or $\alpha_4 \equiv \alpha_3 + 3 \pmod{6}$ then we return to the previous item. Therefore we may assume $\alpha_4 \equiv \alpha_3 + 2 \pmod{6}$. Taking the products $xy^{\alpha_i} \cdot xy^{\alpha_j} = y^{\alpha_j - \alpha_i}$, we can get any element in $\{y, y^2, y^3, y^4, y^5\}$. For example,

$$\begin{aligned} xy^{\alpha_1} \cdot xy^{\alpha_2} &= y, \\ xy^{\alpha_1} \cdot xy^{\alpha_3} &= y^2, \\ xy^{\alpha_2} \cdot xy^{\alpha_4} &= y^3, \\ xy^{\alpha_1} \cdot xy^{\alpha_4} &= y^4, \text{ and} \\ xy^{\alpha_2} \cdot xy^{\alpha_3} &= y^5. \end{aligned}$$

Let i, j such that $\alpha_i - \alpha_j \equiv t_1 \pmod{6}$. Then

$$xy^{\alpha_i} \cdot xy^{\alpha_j} \cdot y^{t_1} = y^{\alpha_j - \alpha_i + t_1} = 1.$$

- **Subcase $k = 5$:** Let $S = (y^t, xy^{\alpha_1}, xy^{\alpha_2}, \dots, xy^{\alpha_5})$. In this case, there are four consecutive α_i 's modulo 6, say $\alpha_1 + 3 \equiv \alpha_2 + 2 \equiv \alpha_3 + 1 \equiv \alpha_4 \pmod{6}$. Then

$$xy^{\alpha_1} \cdot xy^{\alpha_2} \cdot xy^{\alpha_3} \cdot xy^{\alpha_4} = y^{\alpha_2 - \alpha_1 + \alpha_4 - \alpha_3} = 1.$$

- **Subcase $k = 6$:** The only possibility is $S = (x, xy, xy^2, xy^3, xy^4, xy^5)$. So

$$x \cdot xy \cdot xy^3 \cdot xy^2 = 1.$$

□

4. PROOF OF THEOREM 1.4 IN THE CASE $n \geq 4$

We just need to prove that $(i) \implies (ii)$. Let S be a sequence in Q_{4n} with $2n$ elements that is free of product-1 subsequences. We consider some cases depending on the cardinality of $S \cap H_Q$:

- (5.1) **Case $|S \cap H_Q| = 2n$:** In this case, S is contained in the cyclic subgroup of order $2n$. Since $D(H_Q) = D(\mathbb{Z}_{2n}) = 2n$, S contains some non-empty subsequence with product 1.
- (5.2) **Case $|S \cap H_Q| = 2n - 1$:** In this case, by Theorem 2.2, the elements of $S \cap H_Q$ must all be equal, say, $S \cap H_Q = (y^t)^{2n-1}$ where $\gcd(t, 2n) = 1$, and so $S = (y^t)^{2n-1}(xy^s)$.
- (5.3) **Case $|S \cap H_Q| = 2n - 2$:** In this case, let S_1 be a subsequence of S such that $|S_1 \cap H_Q| = n - 2$ and let $S_2 = SS_1^{-1}$. Then S_2 is a sequence in H_Q with n elements. Since

$$Q_{4n}/\{1, y^n\} \simeq D_{2n},$$

Theorem 1.3 tells us that S_1 and S_2 must contain subsequences T_1 and T_2 , respectively, with products in $\{1, y^n\}$. If some of these products is 1 then we are done. Otherwise, both products are y^n , therefore

$$\prod_{z \in T_1 T_2} z = y^{2n} = 1,$$

thus S is not free of product-1 subsequences.

- (5.4) **Case $|S \cap H_Q| = 2n - 3$:** In this case, let S_1 be a subsequence of S such that $|S_1 \cap H_Q| = n - 3$ and let $S_2 = SS_1^{-1}$. Then S_2 is a sequence in H_Q with n elements. The argument is similar to the above case, thus S is not free of product-1 subsequence.

- (5.5) **Case** $|S \cap H_Q| = 2n - k, 4 \leq k \leq 2n$: In this case, let S_1 be a subsequence of S such that $|S_1 \cap H_Q| \leq n - 2$ and $S_2 = SS_1^{-1}$ is such that $|S_2 \cap H_Q| \leq n - 2$. The argument is similar to the above cases, thus S is not free of product-1 subsequence.

Therefore, the proof for $n \geq 4$ is complete. \square

5. PROOF OF THEOREM 1.4 IN THE CASE $n = 3$

We have $Q_{12} = \langle x, y \mid x^2 = y^3, y^6 = 1, yx = xy^5 \rangle$ and we just need to prove that (i) \implies (ii). Let S be a sequence in Q_{12} with 6 elements that is free of product-1 subsequences. We consider some cases depending on the cardinality of $S \cap H_Q$:

- (6.1) **Case** $|S \cap H_Q| = 6$: In this case, S must contain a product-1 subsequence, since $D(H_Q) = D(\mathbb{Z}_6) = 6$.
- (6.2) **Case** $|S \cap H_Q| = 5$: In this case, Theorem 2.2 says that $S \cap H_Q = (y^r)^5$ where $r \in \{1, 5\}$, therefore S is of the form $(y^r)^5(xy^s)$.
- (6.3) **Case** $|S \cap H_Q| = 4$: In this case, we decompose $S = S_1S_2$ where $|S_i| = 3$ for $i \in \{1, 2\}$, $|S_1 \cap H_Q| = 1$ and $|S_2 \cap H_Q| = 3$, and use the same argument than item (5.3), therefore S is not free of product-1 subsequences.
- (6.4) **Case** $|S \cap H_Q| = 3$: In this case, we decompose $S = S_1S_2$ where $|S_i| = 3$ for $i \in \{1, 2\}$, $|S_1 \cap H_Q| = 1$ and $|S_2 \cap H_Q| = 2$, therefore

$$\begin{aligned} S_1 \pmod{\{1, y^3\}} &= (y^r, xy^u, xy^v) \text{ and} \\ S_2 \pmod{\{1, y^3\}} &= (y^t, y^t, xy^s) \text{ for } r, t \in \{1, 2\} \text{ and } s, u, v \in \{0, 1, 2\}. \end{aligned}$$

Notice that S_1 contains a subsequence with product in $\{1, y^3\}$. Observe that if $r \neq t$ then we could also decompose $S = S'_1S'_2$ where

$$S'_1 = S_1(y^t)(y^r)^{-1} \quad \text{and} \quad S'_2 = S_2(y^r)(y^t)^{-1}.$$

So, S'_1 and S'_2 have subsequences with products in $\{1, y^3\}$ and we can use the same argument than item (5.3). Therefore, $r = t$ and we can decompose $S = S''_1S''_2$ such that

$$S''_1 \pmod{\{1, y^3\}} = (y^t)^3 \quad \text{and} \quad S''_2 \pmod{\{1, y^3\}} = (xy^s, xy^u, xy^v).$$

Notice that S''_1 contains a subsequence with product in $\{1, y^3\}$ and S''_2 does not contains a subsequence with product in $\{1, y^3\}$ if and only if $S''_2 \pmod{\{1, y^3\}} = (x, xy, xy^2)$. Hence, the only possibility for $S \pmod{\{1, y^3\}}$ is:

$$S \pmod{\{1, y^3\}} = (y^t)^3(x, xy, xy^2),$$

and so the possibilities for $S \cap H_Q$ are

$$(y)^3, (y^2)^3, (y^4)^3, (y^5)^3, (y)^2(y^4), (y)(y^4)^2, (y^2)^2(y^5) \text{ or } (y^2)(y^5)^2.$$

Notice that the second, third, fifth and seventh possibilities contain subsequences with product 1, therefore it only remains

$$(y)^3, (y^5)^3, (y)(y^4)^2 \text{ or } (y^2)(y^5)^2.$$

Observe that in every case, it is possible to find a subsequence with product either y or y^5 . We claim that $S \cap N_Q$ contains subsequences with product y and y^5 , which we can join with those y or y^5 coming from $S \cap H_Q$ to get a product-1 subsequence. For this, a sufficient condition is the existence of two elements in $S \cap N_Q$ such that the exponents of y have difference 2, since $xy^\alpha \cdot xy^{\alpha+2} = y$ and $xy^{\alpha+2} \cdot xy^\alpha = y^5$. In fact, if $xy^\beta \in S \cap N_Q$ and $xy^{\beta-2}, xy^{\beta+2} \notin S \cap N_Q$ then $xy^{\beta+1}, xy^{\beta-1} \in S \cap N_Q$, and so $(\beta+1) - (\beta-1) = 2$.

- (6.5) **Case** $|S \cap H_Q| = 2$: In this case, we decompose $S = S_1S_2$ where $|S_i| = 3$ and $|S_i \cap H_Q| = 1$, and use the same argument than item (5.3), therefore S is not free of product-1 subsequences.
- (6.6) **Case** $|S \cap H_Q| = 1$: In this case, we decompose $S = S_1S_2$ where $|S_i| = 3$, $|S_1 \cap H_Q| = 1$ and $|S_2 \cap H_Q| = 0$. Notice that S_2 contains a subsequence with product in $\{1, y^3\}$. The same argument than item (5.3) does not apply if and only if $S_2 \pmod{\{1, y^3\}} = (x, xy, xy^2)$. Observe that we could also decompose $S = S'_1S'_2$ in such way that $|S'_i| = 3$ for $i \in \{1, 2\}$, $|S'_1 \cap H_Q| = 1$, $|S'_2 \cap H_Q| = 0$ and $S'_2 \pmod{\{1, y^3\}}$ contains two elements with the same exponent in y . Therefore, the same argument than item (5.3) applies for S'_1 and S'_2 .

- (6.7) **Case** $|S \cap H_Q| = 0$: In this case, we decompose $S = S_1 S_2$ where $|S_i| = 3$ and $|S_i \cap H_Q| = 0$ for $i \in \{1, 2\}$. Notice that S_i contains a subsequence with product in $\{1, y^3\}$ if and only if $S_i \pmod{\{1, y^3\}}$ is not of the form (x, xy, xy^2) . Hence, the same argument than item (5.3) does not apply if and only if $S_i \pmod{\{1, y^3\}} = (x, xy, xy^2)$ for $i \in \{1, 2\}$. Observe that we could also decompose $S = S'_1 S'_2$ in such way that $S'_1 \pmod{\{1, y^3\}} = (x, x, xy)$ and $S'_2 \pmod{\{1, y^3\}} = (xy, xy^2, xy^2)$. Therefore, the same argument than item (5.3) applies for S'_1 and S'_2 .

Therefore, the proof for $n = 3$ is complete. \square

6. PROOF OF THEOREM 1.4 IN THE CASE $n = 2$

We have $Q_8 = \langle x, y \mid x^2 = y^2, y^4 = 1, yx = xy^3 \rangle$. Suppose that S is a sequence in Q_8 with 4 elements that is free of product-1 subsequences. We want to show that S has some of those forms given in item (2). For this, we consider some cases depending on the cardinality of $S \cap H_Q$:

- (7.1) **Case** $|S \cap H_Q| = 4$: In this case, S must contain a product-1 subsequence, since $D(H_Q) = D(\mathbb{Z}_4) = 4$.
- (7.2) **Case** $|S \cap H_Q| = 3$: In this case, Theorem 2.2 says that $S \cap H_Q = (y^r)^3$ where $r \in \{1, 3\}$, therefore S is of the form $(y^r)^3(xy^s)$.
- (7.3) **Case** $|S \cap H_Q| = 2$: In this case, the only possibilities for $S \cap H_Q$ making S be free of product-1 subsequences are

$$(y)^2, (y, y^2), (y^3)^2 \quad \text{and} \quad (y^2, y^3),$$

and in all these possibilities $S \cap H_Q$ possesses a subsequence with product y^2 , namely $y \cdot y, y^3 \cdot y^3$ or y^2 itself. On the other hand, the possibilities for $S \cap N_Q$ are

$$(x, xy), (x, xy^2), (x, xy^3), (xy, xy^2), (xy, xy^3), (xy^2, xy^3) \quad \text{and} \quad (xy^s, xy^s)$$

for $s \in \mathbb{Z}_4$.

The cases (xy^s, xy^s) can be eliminated, since $xy^s \cdot xy^s \cdot y^2 = 1$.

The cases (x, xy^2) and (xy, xy^3) can also be eliminated, since $xy^s \cdot xy^{s+2} = 1$.

The other cases can be eliminated by the following table:

$S \cap N_Q \backslash S \cap H_Q$	$(y)^2$	(y, y^2)	$(y^3)^2$	(y^2, y^3)
(x, xy)	$x \cdot xy \cdot y = 1$	$x \cdot xy \cdot y = 1$	$xy \cdot x \cdot y^3 = 1$	$xy \cdot x \cdot y^3 = 1$
(x, xy^3)	$x \cdot y \cdot xy^3 = 1$	$x \cdot y \cdot xy^3 = 1$	$x \cdot xy^3 \cdot y^3 = 1$	$x \cdot xy^3 \cdot y^3 = 1$
(xy, xy^2)	$xy \cdot xy^2 \cdot y = 1$	$xy \cdot xy^2 \cdot y = 1$	$xy^2 \cdot xy \cdot y^3 = 1$	$xy^2 \cdot xy \cdot y^3 = 1$
(xy^2, xy^3)	$xy^2 \cdot xy^3 \cdot y = 1$	$xy^2 \cdot xy^3 \cdot y = 1$	$xy^3 \cdot xy^2 \cdot y^3 = 1$	$xy^3 \cdot xy^2 \cdot y^3 = 1$

- (7.4) **Case** $|S \cap H_Q| = 1$: In this case, the possibilities for $S \cap H_Q$ are (y) , (y^2) and (y^3) . On the other hand, $S \cap N_Q$ has three elements and, by Equation 2.2, we may assume that $x \in S$. Thus, the possibilities for $S \cap N_Q$ are

$$(x, x, x), (x, x, xy), (x, x, xy^2), (x, x, xy^3), (x, xy, xy), (x, xy, xy^2), (x, xy, xy^3), \\ (x, xy^2, xy^2), (x, xy^2, xy^3) \text{ and } (x, xy^3, xy^3).$$

If S contains (x, xy^2) or (xy, xy^3) then S is not free of product-1 subsequences, since

$$x \cdot xy^2 = 1 = xy \cdot xy^3. \quad (6.1)$$

Therefore, the remainder possibilities are (x, x, x) , (x, x, xy) , (x, x, xy^3) , (x, xy, xy) and (x, xy^3, xy^3) . Notice that these last four possibilities contains two identical terms and two terms such that the exponents of y have difference 1 modulo 4. Since

$$xy^\alpha \cdot xy^{\alpha+1} \cdot y = 1$$

$$xy^\alpha \cdot xy^\alpha \cdot y^2 = 1$$

$$xy^{\alpha+1} \cdot xy^\alpha \cdot y^3 = 1,$$

we may discard these four cases. Therefore, the only remainder possibility is (x, x, x) , and so $S = (y)(xy^s)^3$ or $S = (y^3)(xy^s)^3$.

- (7.5) **Case** $|S \cap H_Q| = 0$: In this case, we also may assume $x \in S$. Therefore, the possibilities for S are

$$\begin{aligned}
& (x, x, x, x), (x, x, x, xy), (x, x, x, xy^2), (x, x, x, xy^3), (x, x, xy, xy), (x, x, xy, xy^2), \\
& (x, x, xy, xy^3), (x, x, xy^2, xy^2), (x, x, xy^2, xy^3), (x, x, xy^3, xy^3), (x, xy, xy, xy), \\
& (x, xy, xy, xy^2), (x, xy, xy, xy^3), (x, xy, xy^2, xy^2), (x, xy, xy^2, xy^3), \\
& (x, xy^2, xy^2, xy^2), (x, xy^2, xy^2, xy^3), (x, xy^2, xy^3, xy^3) \text{ and } (x, xy^3, xy^3, xy^3).
\end{aligned}$$

If S contains two pairs of identical elements, say $(x, x, x^\alpha, x^\alpha)$, then

$$x \cdot x \cdot xy^\alpha \cdot xy^\alpha = 1,$$

so we remove (x, x, x, x) , (x, x, xy, xy) , (x, x, xy^2, xy^2) and (x, x, xy^3, xy^3) .

If S contains some of the pairs (x, xy^2) or (xy, xy^3) then, by equations in 6.1, we may remove other 11 possibilities, thus it only remains (x, x, x, xy) , (x, x, x, xy^3) , (x, xy, xy, xy) and (x, xy^3, xy^3, xy^3) . Therefore, $S = (xy^s)(xy^{r+s})^3$ for $r \in \mathbb{Z}_4^*$ and $s \in \mathbb{Z}_4$. □

Acknowledgements. The second author would like to thank *CAPES/Brazil* for the PhD student fellowship.

REFERENCES

- [1] Adhikari, S. D. *et al*; *Contributions to zero-sum problems*. Discrete Mathematics **306** (2006), 1-10.
- [2] Bass, J.; *Improving the Erdős-Ginzburg-Ziv theorem for some non-abelian groups*. J. Number Theory **126** (2007), 217-236.
- [3] Bovey, J. D., Erdős, P., Niven, I.; *Conditions for a zero sum modulo n* . Canad. Math. Bull. Vol. **18** (1), (1975), 27-29.
- [4] Brochero Martínez, F. E., Ribas, Sávio; *Extremal product-one free sequences in $C_q \rtimes_s C_m$* . (2017), Submitted to "Journal of Pure and Applied Algebra". Available at <https://arxiv.org/pdf/1610.09870.pdf>.
- [5] Caro, Y.; *Zero-sum problems – A survey*. Discrete Mathematics **152**, (1996) 93-113.
- [6] Erdős, P., Ginzburg, A., Ziv, A.; *Theorem in the additive number theory*. Bull. Res. Council Israel **10** (1961) 41-43.
- [7] Gao, W., Geroldinger, A.; *On long minimal zero sequences in finite abelian groups*. Period. Math. Hungar. **38** (3) (1999), 179-211.
- [8] Gao, W., Geroldinger, A.; *On zero-sum sequences in $\mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$* . Integers: Electronic Journal of Combinatorial Number Theory **3** (2003), #A8.
- [9] Gao, W., Geroldinger, A.; *Zero-sum problems in finite abelian groups: a survey*. Expo. Math. **24** (2006), 337-369.
- [10] Gao, W., Geroldinger, A., Gryniewicz, D. J.; *Inverse zero-sum problems III*. Acta Arithmetica. **141.2** (2010), 103-152.
- [11] Gao, W., Geroldinger, A., Schmid, W. A.; *Inverse zero-sum problems*. Acta Arithmetica. **128.3** (2007), 245-279.
- [12] Nathanson, M. B.; *Additive Number Theory*. Springer, New York (1996).
- [13] Olson, J.; *A combinatorial problem on finite Abelian groups I*. J. Number Theory **1** (1969), 8-10.
- [14] Olson, J.; *A combinatorial problem on finite Abelian groups II*. J. Number Theory **1** (1969), 195-199.
- [15] Reiher, C.; *A proof of the theorem according to which every prime number possesses Property B*. Ph.D. thesis, University of Rostock (2010). Available at http://ftp.math.uni-rostock.de/pub/preprint/2010/pre10_01.pdf.
- [16] Schmid, W. A.; *Inverse zero-sum problems II*. Acta Arith. **143** (2010), no. 4, 333-343.
- [17] Schmid, W. A.; *The inverse problem associated to the Davenport constant for $C_2 \oplus C_2 \oplus C_{2n}$, and applications to the arithmetical characterization of class groups*. The Electronic Journal of Combinatorics **18** (2011), #P33 477-487.
- [18] Vosper, A. G.; *The critical pairs of subsets of a group of prime order*. J. London Math. Soc. **31** (1956), 200-205.
- [19] Zhuang, J., Gao, W.; *Erdős-Ginzburg-Ziv theorem for dihedral groups of large prime index*. European J. Combin. **26** (2005), 1053-1059.

DEPARTAMENTO DE MATEMÁTICA, UNIVERSIDADE FEDERAL DE MINAS GERAIS, UFMG, BELO HORIZONTE, MG, 30123-970, BRAZIL,

E-mail address: fbrocher@mat.ufmg.br

E-mail address: savio.ribas@gmail.com